Non-Agentic AI Govenance Singapore

SOVEREIGN STEWARD™ No. 29 · TEACH™
Non-Agentic AI 2.0™ Eldercare Canon

How to Read the Sacred Pause™

Edwin Koh Wui Kiat

Foreword: Why Hardware Governance Matters

The Sacred Pause™ is not a name for a concept. It is a hardware component — a timing gate burned into the bitstream of an FPGA chip — with a specific electrical function: to prevent any downstream signal from propagating until a deterministic delay has elapsed and human-present conditions have been verified.

This e-book teaches the technical reader — the Synapxe engineer, the HSA medical device reviewer, the clinical AI architect — how to read the Sacred Pause™ as a hardware specification, not as a governance metaphor.

> "Policy can be ignored. Hardware cannot. The FPGA delay is as immutable as the speed of light."

Chapter 1: System Overview — The Signal Chain

Architecture Statement

All safety-relevant behaviour in the NGEyeCare™ system is implemented in deterministic, inspectable components: LiDAR sensor → Jetson Thor edge compute → FPGA gate → PLC Sovereign Brake → nurse-call relay. Any AI model or LLM runs as an advisory narrative layer only and has no control lines to any actuator or clinical system.

Layer	Component	Function
Sensing	Livox LiDAR WM003™	96-point voxel cloud, 20Hz, no camera, no audio
Compute	Nvidia Jetson Thor	Postural delta analysis, state classification
Gate	FPGA Sacred Pause™	25–1000ms immutable delay, event hold
Brake	PLC P-002 Sovereign Brake	Tripartite auth enforcement, actuator control
Output	Nurse-call relay / HL7 FHIR	Alert only after all gate conditions met
Advisory	LLM (Claude/Gemini/local)	Narrative text only — no control lines

The Non-Agentic Rule

Every component in the chain above the FPGA is observable but not authoritative. The Jetson classifies postural states. The FPGA holds the classification. The PLC decides whether to actuate. The clinician authorises the PLC. The LLM narrates — it has no access to GPIO, no PLC connection, no NEHR write path.

Chapter 2: The LiDAR Signal Chain

Sensor Hardware

- Sensor: Livox-class LiDAR, fixed-mount, room-scale, 20 Hz scan rate.
- Output: 3D point cloud, down-sampled and quantised into a fixed-size voxel grid (96-cell vector).
- No RGB imaging. No infrared face detection. No embedded microphone. No audio capture path.

Signal Path: Raw → Geometric State

```
Step 1: LiDAR emits pulses → returns captured by sensor ASIC
Step 2: Embedded MCU performs range-gate filtering + static background subtraction
Step 3: Filtered point cloud serialised via shielded LVDS / USB 3.x link → Jetson Thor
Step 4: Jetson C++ deterministic module performs:
         ├── Voxelisation → 96-cell occupancy grid
         ├── Postural state classification: {vertical, transitional, floor-level}
         └── Time-series fall detection: standing → floor within threshold T
```

At the end of Step 4, the system holds one of two states: "fall event pending" or "no event." It does not hold identity. It does not hold a diagnosis. It holds a geometric state transition.

Zero Camera — Technical Implementation

The system achieves Zero Camera not through policy but through sensor physics. The Livox LiDAR operates in the near-infrared band (905nm) and measures time-of-flight to generate distance geometry. It produces a point cloud — a set of (x, y, z) coordinates — not an image. There is no CCD or CMOS imaging sensor in the optical path. Visual identity capture is architecturally impossible.

Chapter 3: The Jetson Thor Compute Environment

Hardened OS Configuration

- Minimal hardened Linux image — only processes required for NGEyeCare™ are running.
- All NGEyeCare™ processes run under a dedicated isolated user with SELinux/AppArmor MAC profile.
- No Wi-Fi stack enabled. No external network interfaces configured.
- Permitted local interfaces only: UART/CAN/GPIO to PLC · HDMI for console · USB (physically keyed, disabled in normal operation).

Memory and Data Handling

- Ring buffer in RAM holds the last N seconds of voxel grids (configurable retention window).
- Optional on-device encrypted scratch storage for audit logs — bounded to 24 hours maximum.
- Purge daemon enforces 24-hour deletion of all non-log data.

— Audit logs are event-level only: {timestamp, anonymised postural state, decision outcome}. No patient identity. No raw sensor data.

Network Isolation — Zero Cloud Technical Specification

There is no TCP/IP route out of the Jetson box during normal operation. Any remote management requires:

— Physical console access — direct HDMI/keyboard connection.
— Authenticated maintenance procedure — access log recorded locally.
— All maintenance access logged for sovereignty audit review.

The only permitted external data channel is a dry-contact relay closure to the hospital nurse-call system, or a locally-routed HL7/FHIR message on a private VLAN — and only after all FPGA + PLC + .1x Key conditions have been satisfied.

Chapter 4: The FPGA Sacred Pause™ — Hardware Specification

Physical Placement

The FPGA is wired inline between the Jetson Thor's event-output GPIO pin and the downstream signal lines leading to:

— PLC input line for nurse-call relay actuation.
— Any external notification channel (if used — e.g. local LAN relay inside hospital on isolated VLAN).

Gate Behaviour — Signal Logic

```
Event path:
  Jetson GPIO → "event_pending" HIGH
  FPGA starts hardware timer: 25ms ≤ T ≤ 1000ms (factory-burned, not software-configurable)
  During timer window:
    └── ALL downstream lines held LOW regardless of Jetson state
  At timer expiry:
    ├── Event exposed to local console UI for human review
    └── Event buffer made visible to PLC (not yet actuated)
  PLC actuates ONLY when tripartite auth conditions satisfied (see Ch. 5)
```

Implementation — HDL and Bitstream

The Sacred Pause™ gate is implemented in Hardware Description Language (HDL) and compiled into the FPGA bitstream at manufacturing time. The key properties:

— No run-time register exists to set the delay to zero — the timing constant is embedded in synthesised logic, not in a configurable register.
— The only way to remove the delay is to physically replace or reprogram the FPGA device — which would be detected in the mandatory Sovereignty Audit (10-Point Sovereignty Audit, P-003).

— The gate is stateless with respect to software — Jetson firmware updates cannot affect FPGA gate timing.

> "Governance as Physics: the FPGA delay cannot be removed by a software update, corporate policy change, or budget cut. It is burned into gates, not written into configuration."

Chapter 5: The PLC Sovereign Brake P-002 — Actuation Architecture

Role and Authority

The Programmable Logic Controller (PLC) is the sole authority over any physical actuator in the ward: call bell, indicator light, relay, siren. All Jetson outputs are treated as requests — the PLC decides whether and when to actuate.

Even if Jetson firmware is compromised, the PLC enforces:

— Rate limits: maximum N alert actuations per minute (configurable by clinical governance team, not by AI layer).

— Lockout states: maintenance mode where no external alerts can be issued.

— Brake state: all coils de-energised unless specific tripartite hardware conditions are simultaneously met.

Tripartite Authentication — Wiring Specification

The PLC is wired to three separate independent input circuits. All three must be true within a narrow temporal window (3–5 seconds) for the PLC to close the nurse-call relay.

Auth Point	Hardware	Mechanism
Biology	Iris Scanner Module	Signed "human-present OK" token via secure serial link — expires after 5s
Intent	Console HMI Panel	Industrial fieldbus / direct PLC connection — NOT OS GUI — operator confirmation keypress
Kinetic	Foot Pedal Switch	Dry-contact switch wired directly into PLC digital input — deliberate physical motion required

The tripartite condition is evaluated by the PLC ladder logic:

```
IF (iris_token_valid AND token_age < 5s)
AND (console_confirm = TRUE)
AND (foot_pedal = CLOSED)
WITHIN temporal_window = 3s
THEN close_relay → nurse_call_actuation
```

This makes the Anti-Doppelgänger Lock physical: no software agent — no matter how capable — can satisfy all three conditions simultaneously. Iris scan requires a living biological body. Console confirmation requires cognitive engagement with the specific observation. Foot pedal requires physical presence at the bedside.

Chapter 6: The MCP Bridge and LLM Placement

Where the AI Model Lives

If Synapxe or a deployer wants to attach a large language model (LLM) — Claude, Gemini, or a local Qwen via LM Studio — it is placed in a separate process or a separate machine, behind a strict interface layer called the Model Context Protocol (MCP) server.

MCP Interface Specification

Direction	Permitted Data	Prohibited Data
LiDAR → LLM	Structured anonymised event summaries: {time, room, geometric state, basic metadata}	Raw sensor feeds, point cloud data, any identifying information
LLM → Clinical	Human-readable text only: "Possible postural event in Bed 3, please review"	GPIO commands, PLC signals, NEHR writes, nurse-call triggers
LLM → Audit	Documentation drafts, structured summaries	Any clinical order, any actuator command

Technical Constraint: LLM Has No Control Lines

- The LLM has no GPIO access.
- The LLM cannot send messages to the nurse-call system.
- The LLM cannot write to NEHR or any clinical order system.
- All LLM outputs are display-only — shown on screen or printed.

From a hardware perspective, the LLM is a "typewriter process" — it produces text and nothing else. It is advisory, not authoritative.

> "LLMs narrate. The LiDAR detects. The FPGA holds. The PLC brakes. The clinician decides."

Chapter 7: Sovereignty Audit Protocol

The 10-Point Sovereignty Audit

Before any ward deployment and after any maintenance event, the following 10-point audit must be passed:

Audit Point	What is Verified
1. Orange Code Cap	Jetson process CPU/memory ceiling confirmed active at 1.1x threshold
2. FPGA Timing	Sacred Pause™ delay confirmed at factory-set value (oscilloscope verification)
3. Zero Camera	No optical imaging device present in sensor hardware manifest
4. Zero Audio	No microphone hardware in device manifest; audio driver absent from OS
5. Zero Cloud	No TCP/IP route to internet; no cloud endpoints in system config
6. 24-Hour Purge	Purge daemon active; last confirmed purge timestamp within 24h
7. PLC Logic	Tripartite auth ladder logic verified — no bypass conditions present
8. Iris Module	Iris scanner signing key valid; token expiry set to ≤5s
9. Foot Pedal	Dry-contact wiring continuity confirmed; pedal NOT in latched state
10. LLM Isolation	LLM process confirmed in separate network namespace; no GPIO/PLC access

Any audit failure triggers an automatic block — the system is locked in maintenance mode until the failed point is cleared and the full audit is re-run. No partial deployment is permitted.

Edwin Koh Wui Kiat (Tiger) · Founding Father, Non-Agentic AI 2.0™
ACRA T260229801 · Patent SG020603109STW · · Singapore ·